AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions of claims in the application:

Listing of Claims:

1. (Currently Amended) An automation security system, comprising:

a processor operatively coupled to memory configured to support the operation of:

an asset component that ~~defines an industrial automation device~~ describes a grouping of one or more factory components to be secured, wherein the grouping of one or more factory components has a severity attribute including at least one of risk and security incident cost;

an access component that defines a security attribute associated with the grouping of one or more factory components to be secured ~~the industrial automation device~~, the security attribute including a location attribute and a time attribute, wherein the time attribute defines direct communication access to the grouping of one or more factory components to be secured ~~industrial automation device~~ for a predetermined amount of time; and

a security component that regulates initial and continuing direct communication access to the grouping of factory components to be secured ~~industrial automation device~~ based upon the security attribute, wherein the security component monitors continuing direct communication and alters or discontinues direct communication access when a security issue arises or is detected.

2-3. (Canceled).

4. (Previously presented) The system of claim 1, the security component is based on at least one of automation and process control security, cryptography, or Authentication/ Authorization/Accounting (AAA).

5. (Currently Amended) The system of claim 1, ~~the asset component describes at least one of factory components or groupings,~~ the factory components are at least one of sensors, actuators, controllers, I/O modules, communications modules, or human-machine interface (HMI) devices.

6. (Currently Amended) The system of claim 5, the ~~groupings~~ grouping of one or more factory components includes factory components that are grouped into at least one of machines, machines grouped into lines, or lines grouped into facilities.

7. (Cancelled)

8. (Currently Amended) The system of claim [[7]] 1, further comprising an ISA S95 Model for Enterprise to Control System Integration to integrate security aspects across or within respective groupings.

9. (Previously Presented) The system of claim 1, further comprising a set of generic IT components and specification of values for parameters required to assemble and configure the IT components to achieve flexible access to the industrial automation device.

10. (Previously Presented) The system of claim 9, the IT components include at least one of switches with virtual local area network (VLAN) capability, routers with access list capability, firewalls, virtual private network (VPN) termination devices, intrusion detection systems, AAA servers, configuration tools, or monitoring tools.

11. (Original) The system of claim 1, further comprising security parameters and policies that are developed for physical and electronic security for various component types.

12. (Previously presented) The system of claim 11, the security parameters and policies further comprising at least one of integrity algorithms or privacy algorithms.

13. (Previously Presented) The system of claim 1, the security component includes at least one of authentication software, virus detection, intrusion detection, authorization software, attack detection, protocol checker, or encryption software.

14. (Previously Presented) The system of claim 13, the security component at least one of acts as an intermediary between an access system and one or more automation components, or facilitates communications between the access system and the one or more automation components.

15. (Previously Presented) The system of claim 1, the security attributes are specified as part of a network request to gain access to the at least one industrial automation device, the security attributes included in at least one of a group, set, subset, or class.

16. (Previously presented) The system of claim 15, the security component employs at least one authentication procedure or an authorization procedure to process the network request.

17. (Previously Presented) The system of claim 16, further comprising one or more security protocols including at least one of Internet Protocol Security (IPSec), Kerberos, Diffie-Hellman exchange, Internet Key Exchange (IKE), digital certificate, pre-shared key, or encrypted password, to process the network request.

18. (Previously presented) The system of claim 15, further comprising security switch to control network access to a device or network.

19. (Currently Amended) The system of claim 18, further comprising an ~~the~~ access key ~~further comprises~~ that includes at least one of time, location, batch, process, program, calendar, or GPS (Global Positioning Information) to specify local and wireless network locations, to control access to the device or network, wherein the access key is re-issued to alter or discontinue direct communication access when the security issue arises or is detected.

20-23. (Canceled).

24. (Withdrawn) An automation security methodology, comprising:

electronically analyzing an industrial automation device;

programmatically modeling the industrial automation device in accordance with network security considerations, the network considerations include a location attribute and a time attribute that controls if and how long network access is granted to the industrial automation device; and

automatically developing a security framework for an automation system based in part on the modeling of the industrial automation device, a network access type and at least one of a formal threat analysis, a vulnerability analysis, a factory topology mapping, or an attack tree analysis to determine whether access should be granted to the industrial automation device.

25. (Canceled).

26. (Withdrawn) The method of claim 24, the one or more security attributes further comprise at least one of a role, an asset type, a location, a time, or an access type.

27. (Withdrawn) The method of claim 24, further comprising at least one of:
determining whether to grant access to the industrial automation device;
granting access from the industrial automation device; or
granting access from a network device associated with the industrial automation device.

28-33. (Canceled).

34. (Currently Amended) An automated security system, comprising:

a processor coupled to memory, the processor configured to:

define security attributes associated with at least one network request to an industrial automation device, the security attributes include a location attribute and a time attribute and at least one of:

a role attribute, or

an access type attribute;

process the security attributes;

control direct communication access to the industrial automation device based in part on the security attributes;

monitor the direct communication access; and

modify or terminate the direct communication access when a security ~~event~~ problem is detected during the monitor of the direct communication access.

35. (Previously presented) The system of claim 34, wherein control of direct communication access is based on at least one of automation and process control security, cryptography, or Authentication/ Authorization/Accounting (AAA).

36. (Previously presented) The system of claim 34, wherein monitor of direct communication access includes at least one of virus detection, intrusion detection, authorization software, attack detection, or protocol checker.

37. (Previously presented) The system of claim 34, wherein the role attribute includes at least one of an integrator, an original equipment manufacturer (OEM), a supplier, maintenance, an outsourced manufacturer, an engineer, or a user name.

38. (Previously presented) The system of claim 34, wherein the access type attribute includes at least one of status access, read access, write access, read and write access, program update access, program read access, I/O manipulation access, memory location access, or data table access.

39. (Previously presented) The system of claim 34, wherein the time attribute defines how long direct communication access exists.

40. (Previously presented) The system of claim 34, the one or more security attributes are defined in an access key.

41. (Previously presented) The system of claim 40, wherein modify or terminate the direct communication access includes at least one of:

issue a new access key;

alter the access key; or

revoke the access key.

42. (Previously presented) A method for providing automatic security, comprising:

determining security attributes for at least one network request by an entity to an industrial automation apparatus including processing a location security attribute, a temporal security attribute and at least one of a role security attribute or an access type security attribute;

controlling direct communication access to the industrial automation apparatus by the entity as a function of the security attributes;

monitoring the direct communication access by the entity; and

modifying the direct communication access when a security event is detected during the monitoring of the direct communication access.

43. (Previously presented) The method of claim 42, wherein the modifying includes terminating the direct communication access when a security event is detected during the monitoring of the direct communication access.

44. (Previously presented) The method of claim 42, wherein the determining includes defining the security attributes for the at least one network request by the entity.